Linux Network Servers

Instalação de Hardening

Nesse curso vamos falar 100% do tempo sobre servidores Linux. Antes de falarmos de Linux, temos que falar um pouco de hardware, especialmente discos rígidos (hard disk, HD).

Os tipos de discos que existem são:

- IDE/ATA (IDE e ATA são considerados sinônimos)

ATA, um acrônimo para a expressão inglesa **Advanced Technology Attachment**, é um padrão para interligar dispositivos de armazenamento, como discos rígidos e drivers de CD-ROMs.

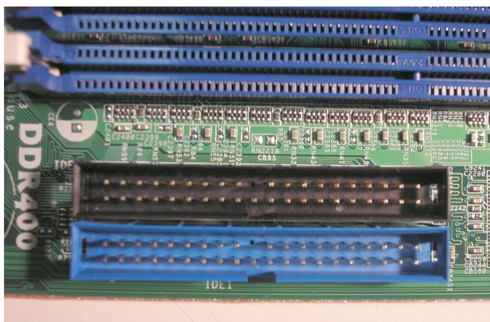


Ilustração 1: Slots IDE



Ilustração 2: Cabo flat

Arquivos-dispositivos:

IDE Primária	Master: /dev/hda
	Slave: /dev/hdb
IDE Secundária	Master: /dev/hdc
	Slave: /dev/hdd

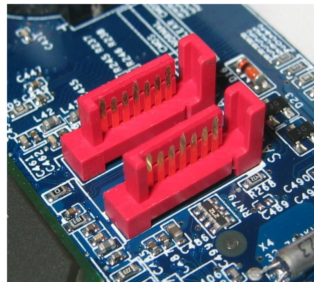


Ilustração 3: Cabo sata

- **Serial ATA**, **SATA** ou **S-ATA** (acrônimo para *Serial Advanced Technology Attachment*) é uma tecnologia de transferência de dados entre um computador e dispositivos de armazenamento em massa (mass storage devices) como unidades de disco rígido e drives ópticos. É o sucessor da tecnologia ATA(acrônimo de *Advanced Technology Attachment* também conhecido como IDE ou *Integrated Drive Electronics*) que foi renomeada para *PATA* (*Parallel ATA*) para se diferenciar de SATA. Diferentemente dos discos rígidos IDE, que transmitem os dados através de cabos de quarenta ou oitenta fios paralelos, o que resulta num cabo enorme, os discos rígidos SATA transferem os dados em série. Os cabos Serial ATA são formados por dois pares de fios (um par para transmissão e outro par para recepção) o que permite usar cabos com menor diâmetro que não interferem na ventilação do gabinete.

Linux Network Servers

As principais vantagens sobre a interface do parallel ATA, é em relação a rapidez em transferir os dados, cuja habilidade é remover ou acrescentar dispositivos enquanto a operação (hot swapping) de cabos mais finos que permite o resfriamento de ar mais eficientemente e, uma operação mais confiável, com dados controlados vigorosamente. Designado como um sucessor para o padrão ATA (Advanced Technology Attachment), o qual eventualmente se espera substituir a tecnologia mais antiga, retroativamente com o nome(Parallel ATA ou PATA), os quais se denominam adaptadores e dispositivos do Serial ATA de comunicação de alta velocidade, ao longo de um serial cable.


Ilustração 4: Slots sata

Arquivos-dispositivo:

Sata	/dev/sdX , onde X depende da quantidade de dispositivos (observação: sdX pode representar outros dipositivos USB). Exemplos: /dev/sda, /dev/sdb, /dev/sdc

Dica: No Linux, dispositivos Sata e Scsi são vistos da "mesma forma" (nomenclatura de arquivos dispositivos).

cd /proc/scsi

cat scsi

Attached devices:
Host: scsi0 Channel: 00 Id: 00 Lun: 00
  Vendor: ATA   **Model: SAMSUNG HD160JJ**/ Rev: ZM10
  Type: Direct-Access   ANSI SCSI revision: 05
Host: **scsi0** Channel: 00 Id: 01 Lun: 00
  Vendor: **TSSTcorp Model: CDDVDW SH-S223F** Rev: SB00
  Type: CD-ROM   ANSI SCSI revision: 05
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor: **MAXTOR S Model: TM3500320AS**   Rev:
  Type: Direct-Access   ANSI SCSI revision: 02

Linux Network Servers

- **SCSI**

Pronuncia-se "scuzi", sigla de Small Computer System Interface, é uma tecnologia que permite ao usuário conectar uma larga gama de periféricos, tais como discos rígidos, unidades CD-ROM, impressoras e scanners. Características físicas e elétricas de uma interface de entrada e saída (E/S) projetadas para se conectarem e se comunicarem com dispositivos periféricos são definidas pelo SCSI.

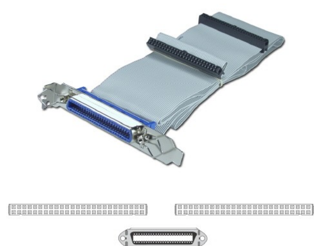


Ilustração 6: Cabos SCSI



Ilustração 5: Controladora SCSI

Existe uma grande variedade de padrões de dispositivos SCSI, sendo que estes inicialmente usavam interfaces paralelas. Alguns exemplos: SCSI-1 (barramento de 8 bits, clock de 5 MHz e taxa de transferência de 5 MB/s), Fast SCSI (barramento de 8 bits, clock de 10 MHz e taxa de transferência de 10 MB/s), Ultra SCSI (barramento de 8 bits, clock de 20 MHz e taxa de transferência de 20 MB/s), Ultra2 Wide SCSI (barramento de 16 bits, clock de 40 MHz e taxa de transferência de 80 MB/s) e Ultra-320 SCSI (barramento de 16 bits, clock de 80 MHz DDR e taxa de transferência de 320 MB/s).

Posteriormente foram também criadas interfaces seriais, como a SSA (Serial Storage Architecture), com taxa de transferência de 40 Mb/s e SAS (Serial Attached SCSI) de 300 Mb/s, também chamado de SASCSI.

Linux Network Servers

- **Solid state**

SSD, sigla do inglês *solid-state drive*, que significa unidade de estado sólido, é um tipo de dispositivos sem partes móveis para armazenamento não volátil de dados digitais. Tipicamente, são construídos em torno de um circuito integrado semicondutor, o qual é responsável pelo armazenamento, diferentemente, portanto, dos sistemas magnéticos (HD) ou óticos (CD). Alguns dos dispositivos mais importantes usam memória RAM, e há ainda os que usam memória flash.

Os dispositivos SSD têm características que constituem vantagens sobre dispositivos de armazenamento convencionais. Entre elas:

1. tempo de acesso reduzido, uma vez que o acesso à memória RAM é muito menor do que o tempo de acesso a meios magnéticos (como os HDs) ou ópticos (discos como Cds e DVDs). Outros meios de armazenamento sólidos podem ter características diferentes;
2. eliminação de partes móveis eletro-mecânicas, o que reduz vibrações e os torna completamente silenciosos;
3. por não possuírem partes móveis são muito mais resistentes que os HDs comuns, contra choques mecânicos, o que é extremamente importante quando se fala em computadores portáteis;
4. menor peso em relação aos discos rígidos, mesmo os mais portáteis;
5. consumo reduzido de energia;
6. possibilidade de trabalhar em temperaturas maiores que os HDs comuns - cerca de 70ºC;
7. banda muito superior aos demais dispositivos, com dispositivos apresentando 250MB/s na gravação e até 700MB/s nas operações de leitura;

As taxas de transferência (na maioria dos modelos) são equivalentes a de um HD modesto, em sistemas de alto desempenho, o critério de alta velocidade de acesso é o mais importante, além de reduzir bastante o tempo de boot, mas no caso de dispositivos de baixo consumo de energia, ou baixo custo, o critério da redução do consumo de energia é o mais importante. Porém, para os padrões atuais de mercado e aplicação os dispositivos SSD ainda são bastante caros se comparados a dispositivos magnéticos, para solucionar este problema, atualmente estão sendo lançados discos híbridos, contendo aproximadamente 2GB em Flash mais um disco convencional.

Dica!
Um comando interessante de ser usado é o comando hdparm, que mostra o desempenho do disco rígido.

```
# hdparm -t /dev/sda
/dev/sda:
 Timing buffered disk reads:  182 MB in  3.00 seconds =  60.66 MB/sec
```

Veja a velocidade de leitura que foi de 60.66 MB/sec.

Quais características da distribuição são importantes para um servidor?

* atualizações de segurança
* período de suporte
* comunidade
* estabilidade
* variedade de pacotes

Linux Network Servers

Dica de segurança!
Sempre ficar atento a política de atualização de sua distribuição. Opte por uma distribuição com pelo menos 2 anos de suporte de segurança.

Bom, já temos nossa distribuição definida, agora precisamos instalar. Para garantirmos uma boa disponibilidade, facilidade de gerenciamento e segurança, devemos fazer uma instalação do sistema operacional adequada ao perfil do serviço que a máquina vai oferecer. Para isso, precisamos saber pra que serve cada diretório no Linux.

* /bin/ Comandos binários essenciais para todos os usuários (ex: cat, ls, cp)
* /boot/ Arquivos do Boot loader, kernel, initrd.
* /dev/ Dispositivos (ex: /dev/null).
* /etc/ Arquivos de configuração específicos do computador.
* /home/ Diretórios de usuários.
* /lib/ Diretório com as bibliotecas essenciais para os arquivos binários contidos nos diretórios /bin/ e /sbin/.
* /mnt/ Sistemas de arquivos "montados" temporariamente.
* /media/ Pontos de "montagem" para mídia removível, como CD-ROMs.
* /opt/ Pacotes estáticos de aplicações.
* /proc/ Sistemas de arquivo virtual, que possui o estado do Kernel e processos do sistema; a maioria dos arquivos é baseada no formato texto (ex: tempo de execução, rede).
* /root/ Diretório home para o super usuário (root).
* /sbin/ Arquivos binários para propósito de adminstração do sistema.
* /tmp/ Arquivos temporários. (Ver também /var/tmp).
* /srv/ Dados específicos que são servidos pelo sistema.
* /usr/ Hierarquia secundária para dados compartilhados de usuários, cujo acesso é restrito apenas para leitura.
* /var/ Arquivos "variáveis", como logs, base de dados, páginas Web e arquivos de e-mail.

O que é uma partição e quais os tipos?

Uma partição é um espaço do disco que se destina a receber um sistema de arquivos ou, em um caso particular que veremos adiante, outras partições.

Existem três tipos possíveis de partições: primária, estendida e lógica.

Este tipo de partição contém um sistema de arquivos. Em um disco deve haver no mínimo uma e no máximo quatro partições primárias. Se existirem quatro partições primárias, nenhuma outra partição poderá existir neste disco.

Só pode haver uma partição estendida em cada disco. Uma partição estendida é um tipo especial de partição primária que não pode conter um sistema de arquivos. Ao invés disso, ela contém partições lógicas.

As partições lógicas residem dentro da partição estendida. Podem haver de uma a 12 partições lógicas em um disco.

Linux Network Servers

Quais diretórios alocar em partições distintas? Por que?

* /boot Separar o kernel e initrd
* /var Gravação constante. Pode lotar o disco.
* /home Gravação constante. Pode lotar o disco.
* /tmp Todos os usuários podem gravar. Pode lotar o disco.

A integridade do sistema de arquivos fica mais assegurada, pois estão em partições deferentes.

Dica de segurança!
SEMPRE separar /var e /tmp em partições diferentes.

Existe uma fórmula exata para o particionamento?

Não, cada caso é um caso. Temos que analisar o perfil do servidor. Por exemplo, se estamos falando de um firewall precisamos de bastante espaço para o diretório /var/log, se estamos fazendo um servidor de arquivos, usando samba ou nfs, netão precisaremos de uma partição bem grande só para guardar os arquivos dos usuários, separando-os dos arquivos do sistema.

Agora que temos nosso disco particionado temos que formatar essas partições. Qual seria o melhor sistema de arquivos? Porque?

Novamente depende da necessidade, só que temos que usar um sistema de arquivos com journaling. ext3, xfs ou reiserfs.

O que é journaling?

Basicamente, o sistema de arquivos mantém um journal (ou log) onde são armazenadas todas as mudanças feitas em arquivos do disco. Quando qualquer erro inesperado surge, ou o sistema é desligado incorretamente é possível localizar todas as operações que não haviam sido completadas, restaurando a consistência do sistema de arquivos sem a necessidade de vasculhar arquivo por arquivo, como faz o scandisk do Windows ou o FSCK no Linux.

Acesse o seguinte link para ler sobre um benchmark comparando os sistemas de arquivos: ext3, reiserfs, xfs, jfs: http://www.debian-administration.org/articles/388

Linux Network Servers

E quanto deixar de swap (memória virtual)?

A área de swap nada mais é que um espaco no HD para o "depósito" de programas que não estão sendo usados. Isso é, se você tiver 512Mb de memória RAM, e apenas 2 MB livres (você já tem um monte de programas abertos) e quiser abrir o seu Firefox (que ocupa muito mais que 2MB na RAM), o Linux vai jogar o programa que esta a um bom tempo parado para a área de swap e, com o espaço livre na sua RAM, abrir o Firefox.

Há uma regra muito falada por aí que para definir o tamanho dela que é pegar o tamanho da RAM e multiplicar por 2, ou seja, se eu tiver 256 MB de RAM, minha swap deverá ter 512 MB. Mas isso já não serve muito de base mais, pois a quantidade de memória RAM já chegou a escala de giga. Não faria sentido se eu tivesse 4 GB de RAM e atribuísse 8 GB de swap para um desktop por exemplo. Portanto, é necessário ter bom senso. No máximo 2 GB para swap é o necessário. Se você necessita de muita swap, talvez seja necessário colocar mais memória RAM, pois a swap é mais lenta que a RAM. A memória RAM funciona apenas eletronicamente, enquanto o disco rígido é um dispositivo mecânico e eletrônico.

Curiosidade: Para se ter uma idéia, uma memória DDR2 comunica-se com o processador a uma velocidade em torno de 4000 MB por segundo. A leitura de um disco rígido atual gira em torno de 100 MB por segundo.

Temos a distribuição instalada. Ela está pronta pra ser usada?

Hardening é um processo de mapeamento das ameaças, mitigação dos riscos e execução de atividades corretivas, com foco na infra-estrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque. Normalmente, o processo inclui remover ou desabilitar nomes ou logins de usuários que não estejam mais em uso, além de serviços desnecessários.

Outras providências que um processo de hardening pode incluir: limitar o software instalado àquele que se destina à função desejada do sistema; aplicar e manter os patches atualizados, tanto de sistema operacional quanto de aplicações; revisar e modificar as permissões dos sistemas de arquivos, em especial no que diz respeito a escrita e execução; reforçar a segurança do login, impondo uma política de senhas fortes. Temos que fechar nosso sistema o máximo possível, dificultando a ação de um cracker. Segurança nunca é demais.

O primeiro passo que devemos dar ao proteger nosso servidor após uma instalação, é proteger o máximo possível o sistema de arquivos.

O que podemos fazer para melhorar a segurança?

* exec, noexec - Permite ou não a execução de binários no sistema de arquivos.
* rw - Monta o sistema de arquivos com a opção Read-Write, ou seja, leitura e escrita.
* ro - Monta o sistema de arquivos com a opção Read-Only, ou seja, somente leitura.
suid, nosuid - Habilita/desabilita o bit de set-user-identifier ou set-group-identifier.
* dev, nodev - Serve para desabilitar a interpretação de dispostivos de blocos especiais em um sistema de arquivos

Exemplo:
/dev/sda5 /home ext3 defaults,noexec,nodev 0 0
/dev/sda6 /tmp ext3 defaults,noexec,nodev 0 0

Linux Network Servers

Dica de segurança!
Porque no /tmp? Muitos rootkits procuram este tipo de acesso através do /tmp, por isso é recomendado se ter o /tmp em partições diferentes, já que ele é de gravação universal.

Dica de segurança!
Montando o /tmp com noexec você impede que um HACKER jogue programas dentro do /tmp e execute. Isso ajuda a evitar muitos ataques de escalação de privilégios.

E a senha do root, como deve ser?
Deve ser uma senha bem forte, com números, caracteres especiais, letras maiúsculas e minusculas misturadas. Por exemplo: Efae:Z7P Hoo(f4Gu Ud-ah8lo
Dica de segurança!
Use o comando pwgen para gerar suas senhas, ex: pwgen -y

Para isso, instale-o no Debian:
aptitude install pwgen

Se eu tenho uma senha de root forte e eu tenho acesso físico ao servidor, estou seguro?
Não, pois ter acesso físico ao servidor nos permite fazer praticamente qualquer coisa com ele.

Por padrão alguns serviços vem ativados, devemos mantê-los caso não precisamos deles?

Nunca manter serviços e pacotes instalados nos servidor que não sejam extritamente necessários

Precisamos manter nosso servidor sempre atualizado? Por que?

Todo software tem bugs de segurança e é fundamental nos mantermos atualizados. É fundamental que você esteja inscrito em listas de discussão que enviam notificações de segurança para a sua distribuição.

Ex:
http://lists.debian.org/debian-security-announce/
https://rhn.redhat.com/errata/rhel-server-errata.html